UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/618,202	07/18/2000	Kenji Yamagami	16869C008600US	9713

7590 01/05/2005

Robert C Colwell
Townsend and Townsend and Crew LLP
8th Floor
Two Embarcadero Center
San Francisco, CA 94111-3834

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Applicati n No.	Applicant(s)	
	09/618,202	YAMAGAMI ET AL.	
	Examin r	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disp sition of Claims

4)☒ Claim(s) *1-23 and 26-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23 and 26-31* is/are rejected.

7)☒ Claim(s) *17-22 and 27-29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-23 and 26-31 are pending in this office action.

Claim Objections

2. Claims 17-22 and 27-29 are objected to because of the following informalities:

- Claim 17 recites "a second communications link coupling the local system to the remote system," when it should be a **local disk system** to the **remote disk system**.
- Claims 18-22 are dependent on claim 17 and therefore inherit its deficiencies.
- Claim 27 recites "transferring the encrypted data to the remote disk system," when it should be transferring the encrypted data to the remote disk system **via a second communications link**.
- Claims 28-29 are dependent on claim 27 and therefore inherit its deficiencies.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1, 9-17, 23, and 26-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohran (U.S. Patent No. 6,397,307) in view of Yanai et al. (U.S. Patent No. 5,544,347).

Regarding claim 1, Ohran teaches a method of controlling security of data in a storage system having a local disk system and a remote disk system **that are coupled to at least one host computer, the method** comprising:

- In the local disk system **coupled to a first host computer**:
  - When a write of data is to be made to the local disk system retrieving a previously stored encryption key (col. 11, lines 24-26 suggests to use stored encryption keys for encryption, even though the teachings of Ohran dynamically creates an encryption key);
  - Encrypting the data (col. 11, lines 43-45);
  - Transferring the data to the remote disk system **via a first communication link** (col. 11, lines 45-47);
- Then in the remote disk system:
  - Determining an address for storage of the data in the remote disk system (col. 9, lines 29-35 and col. 10, lines 21-27);
  - Writing the data in the remote disk system (col. 9, lines 39-43 and col. 10, lines 21-27);
  - Determining whether the data is to be stored in an encrypted form (col. 11, lines 40-43 suggests that some of the data can be encrypted, but does not necessarily mean the same data has to be decrypted); and
  - If the data is to be stored in a decrypted form, decrypting and writing the data in the remote disk system (col. 11, lines 47-49); and

- If the data is to be stored in an encrypted form, writing the data in the remote disk system without decrypting the data (col. 11, lines 40-43, the word ***may*** suggests that the data does not have to be decrypted).

Ohran does not teach notifying the local disk system **via the first communication link** that the step of writing the data is complete, wherein the local disk system is coupled to **the first** host computer **via a second communication link** to allow the **first** host computer to access data stored in the local disk system, **the first and second communication links being different**.

Yanai et al. teaches notifying the local disk system that the step of writing the data is complete (col. 6, lines 41-46), wherein the local disk system is coupled to **the first** host computer **via a second communication link** to allow the **first** host computer to access data stored in the local disk system, **the first and second communication links being different** (fig. 1, ref. num 40 and 18).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine notifying the local disk system that the step of writing the data is complete, wherein the first and second communication links are different, as taught by Yanai et al., to the method of Ohran. It would have been obvious for such modifications because the notification allows the local disk system to know that the data is synchronized between the local and remote disk system.

Regarding claims 9 and 23, Ohran teaches a method for e... ...ncryption key while operating a storage system having a local disk syste... ...disk system comprising:

- Storing an encryption key in a memory in the local disk sy... ...num 106a);
- Transmitting the encryption key to the remote disk system a... ...in a memory there **via a first communication link coupling (fi... ...remote disk systems** (fig. 6, ref. num 16 and 106b);
- In the local disk system determining a boundary for use of t... ...key (col. 11, lines 52-55 the keys are changed at every time of e...);
- In the remote disk system receiving the boundary from the l... ...stem (fig. 16, ref. num 16);
- In both the local and the remote disk system, determining a... ...of present operations to the boundary (fig. 2, ref. num 30, 36, ...
- In both the local and the remote disk system waiting for the ... ...nd then changing the encryption key for data stored thereafter (fig. ... ...2 and 38 and col. 11, lines 52-55).

Ohran does not specifically teach the encryption key is st... ...l disk and transmitted to the remote disk and stored, wherein the loca... ...is **coupled to a first host computer via a second communicatio... ...different than the first communication link.** Ohran teaches the local di... ...disk

exchange values and calculate a key (the keys being equal), which is stored in the local disk system and remote disk system.

Yanai et al. teaches **wherein the local disk system is coupled to a first host computer via a second communication link that is different than the first communication link** (fig. 1, ref. num 18 and 40).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine altering the key exchange process to include transmitting the stored key from the local system to the remote system, instead of transmitting values to calculate the key, wherein the first and second communication links are different, as taught by Yanai et al., with the method of Ohran. It would have been obvious for such modifications because, as suggested on col. 11, lines 24-26 (Ohran), the keys could already be calculated and stored in the local system. This would save computation time of calculating keys by swapping values between the two systems.

Regarding claim 10, Ohran as modified by Yanai et al. teaches wherein operations before the boundary are performed using a first encryption key and operations after the boundary are performed using a second encryption key (see col. 11, lines 52-55 of Ohran).

Regarding claims 11 and 15, Ohran as modified by Yanai et al. teaches wherein the boundary is defined by counting input/output operations and using the count to define the boundary (see col. 13, lines 35-50 of Ohran uses a decided time T to decide the boundary, and only the last IO operation before a decided time T is transmitted to the remote system).

Regarding claim 12, Ohran teaches a method for changing an encryption key while operating a storage system having a local disk system and a remote disk system, the method comprising:

- Storing an encryption key in a memory in the local disk system (fig. 6, ref. num 106a);
- Transmitting **via a first communication link** the encryption key to the remote disk system and storing it in a memory there (fig. 6, ref. num 16 and 106b);
- Issuing split request from the local disk system to the remote disk system to allow them to operate independently (fig. 2, the time between consolidations the local system is operated independently of the remote system);
- Using a new encryption key to begin storing data in the local disk system after issuing the split request (col. 11, lines 52-55); and
- Using a new encryption key to begin storing data in the remote disk system after receiving the split request (col. 11, lines 52-55).

Ohran does not teach re-synchronizing the local disk system and the remote disk system, **wherein the local disk system is coupled to a host computer via a second communication link that is different than the first communication link to allow the host computer to access data stored in the local disk system, the first and second communication links being different.**

Yanai et al. teaches re-synchronizing the local disk system and the remote disk system (col. 6, lines 38-51), **wherein the local disk system is coupled to a host computer via a second communication link that is different than the first communication link to allow the host computer to access data stored in the local disk system, the first and second communication links being different** (fig. 1, ref. num 18 and 40).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine re-synchronizing the local system and the remote system, wherein the first and second communication links are different, as taught by Yanai et al., to the system of Ohran. It would have been obvious for such modifications because synchronizing the data between the local and remote systems will make sure the remote system has the same data as the local system. This is important in systems where data is mirrored or back ed-up.

Regarding claim 13, Ohran teaches a method of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

- Determining a boundary in the local disk system where encryption is to be switched to an opposite state (col. 11, lines 52-55 the keys are changed at every time of consolidation);
- In the remote disk system receiving a corresponding boundary from the remote disk system (the remote system boundary is the same place that the local system boundary is);
- In both the local and the remote disk system, determining a relationship of present operations to the boundary (fig. 2, ref. num 30, 36, and 42);
- In both the local and the remote disk system waiting for the boundary, and then changing the switching the encryption to the opposite state (fig. 2, ref. num 32 and 38).

Ohran does not teach maintaining a control table in each of the local and remote disk systems, **wherein the local disk system is coupled to a host computer via a first communication link, and the remote disk system is coupled to a second host computer via a second communication link, the local disk system and the remote disk system being coupled to each other via a third communication link, the third communication link being different than the first or second communication link.** Ohran teaches keys (which control encryption) in each system. Also, tables containing data are well known in the art and would be an obvious addition to this system.

Yanai et al. teaches **wherein the local disk system is coupled to a host computer via a first communication link, and the remote disk system is coupled to a second host computer via a second communication link, the local disk system and the remote disk system being coupled to each other via a third communication link, the third communication link being different than the first or second communication link** (fig. 1, ref. num 18, 40, 52, and 54).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine maintaining a control table in each of the local and remote disk systems, wherein the first, second, and third communication links are different, as taught by Yanai et al., with the method of Ohran. It would have been obvious for such modifications because maintaining a control table in the local and remote disk system supplies data values to the disk systems telling them how to respond to data.

Regarding claim 14, Ohran as modified by Yanai et al. teaches wherein operations before the boundary are either encrypted or not encrypted, and operations performed after the boundary are either not encrypted or encrypted oppositely to those operations performed before the boundary (see col. 11, lines 40-43 of Ohran, the data can be encrypted at any time and can not be encrypted anytime, it all depends on the users' data).

Regarding claims 16 and 26, Ohran teaches a method/system of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

- Storing an encryption key in a memory in the local disk system **that is coupled to a host computer via a first communication link** (fig. 6, ref. num 106a);
- Transmitting **via a second communication link** the encryption key to the remote disk system and storing it in a memory there (fig. 6, ref. num 16 and 106b);
- Splitting the local disk system from the remote disk system to allow them to operate independently (fig. 2, the time between consolidations the local system is operated independently of the remote system); and
- Switching encryption to an opposite state from a previous state after splitting the local disk system and remote disk system (col. 11, lines 40-43, the data can be encrypted at any time and can not be encrypted anytime, it all depends on the users' data).

Ohran does not teach re-synchronizing the local disk system and the remote disk system, **the first and second communication links being different.**

Yanai et al. teaches re-synchronizing the local disk system and the remote disk system (col. 6, lines 38-51), **the first and second communication links being different** (fig. 1, ref. num 18 and 40).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine re-synchronizing the local system and the remote system, wherein the first and second communication links are different, as taught by Yanai et al., to the system of Ohran. It would have been obvious for such modifications because synchronizing the data between the local and remote systems will make sure the remote system has the same data as the local system. This is important in systems where data is mirrored or backed-up.

Regarding claim 17, Ohran teaches a storage system comprising:

- A local disk system (fig. 1, ref. num 12);
    - Said local disk system being coupled to a host computer **via a first communication link** to enable the host computer to access said volumes (fig. 1, ref. num 20 connected to 12);
- A **second** communications link coupling the local system to the remote system (fig. 1, ref. num 16);
- Wherein the local disk system determines whether encryption is to be employed in the data on the local disk system, and if so, encrypts the data to be transferred to the remote disk system (col. 11, lines 24-26 and 40-45 suggests that some or all of the data ***may*** be encrypted, meaning it does not have to be), and
- Wherein the remote disk system determines whether to store the data in either encrypted form or unencrypted form and stores the data in that form in the

remote disk system (col. 11, lines 24-26 and 40-45 suggests that some or all of the data ***may*** be encrypted, meaning it does not have to be).

Ohran does not teach the local system or remote system including a plurality of volumes of media for storing data and notifying the local disk system that the data has been stored **via the second communication link, wherein the first and second communication links are different.**

Yanai et al. teaches the local system and remote system including a plurality of volumes of media for storing data (fig. 1, ref. num 20 and 48) and notifying the local disk system that the data has been stored **via the second communication link** (col. 6, lines 41-46), **wherein the first and second communication links are different** (fig. 1, ref. num 18 and 40).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the local system including a plurality of volumes of media for storing data and notifying the local disk system that the data has been stored, wherein the first and second communication links are different, as taught by Yanai et al., to the system of Ohran. It would have been obvious for such modifications because the plurality of volumes for storing data allows the local disk system to contain a volume that is local only to it and volumes that are accessible by the remote system (col. 5, lines 11-

34) and the notification allows the local disk system to know that the data is synchronized between the local and remote disk system.

Regarding claim 27, Ohran teaches a method of controlling security of data in a storage system having a local disk system and a remote disk system comprising:

- In the local disk system:
  - Receiving a data update request from a host computer connected to the local disk system wherein said data update request includes a location of a first portion of the local disk system, **the host computer being connected to the local disk via a first communication link** (col. 5, lines 39-52, the local disk system is required to determine update times);
  - Assigning a key to the local disk system (col. 11, lines 43-45);
  - Encrypting the data stored in the local disk system (col. 11, lines 43-45);
  - Transferring the encrypted data to the remote disk system (col. 11, lines 45-47);
- Then in the remote disk system:
  - Decrypting the data using the assigned key (col. 11, lines 47-49); and
  - Writing the decrypted data into the remote disk system (col. 9, lines 39-43 and col. 10, lines 21-27).

Ohran does not teach a first portion of the local disk system or a second portion of the remote disk system, **wherein the first and second communication links are different.**

Yanai et al. teaches a first portion of the local disk system (fig. 1, ref. num 22a) and a second portion of the remote disk system (fig. 1, ref. num 50a), **wherein the first and second communication links are different** (fig. 1, ref. num 18 and 40).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a first portion of the local disk system and a second portion of a remote disk system, wherein the first and second communication links are different, as taught by Yanai et al., to the method of Ohran. It would have been obvious for such modifications because the first and second portions allow the local and remote disk system to contain separate portions that are local only and accessible by the other disk system (col. 5, lines 11-34).

Regarding claim 28, the combination of Ohran as modified by Yanai et al. teaches wherein the first portion comprises at least a volume of the local storage system and the second portion comprises at least a volume of the remote disk system (see fig. 1, ref. num 20 and 48 of Yanai et al.).

Regarding claim 29, the combination of Ohran as modified by Yanai et al. teaches wherein the first portion comprises a group of volumes of the local storage system (fig. 1, ref. num 22a-c of Yanai et al.), and the second portion comprises a group of volumes of the remote storage system (see fig. 1, ref. num 50a-c of Yanai et al.).

Regarding claim 30, Ohran teaches a storage system comprising:

- A local disk system (fig. 1, ref. num 12),
- A remote disk system (fig. 1, ref. num 14);
- A first computer program operating on the local system to retrieve selected data from storage on the local system, and encrypt the selected data using an encryption key (col. 11, lines 43-45);
- Wherein the local disk system retrieves selected data from one of the volumes on the local system, encrypts that selected data using an encryption key, and transmits the encrypted selected data to the remote disk system (fig. 1, ref. num 16, 12, and 20); and
- Wherein the remote disk system decrypts the selected data received from the communications link and store that selected data in unencrypted form in one of the volumes of media the remote system (col. 11, lines 47-49).

Ohran does not teach the local and remote disk system including a plurality of volumes of media for storing data, wherein the local disk system is connected to a host computer **via a first communication link; a second** communications link coupling the

local disk system to the remote disk system, **the first and second communication links being different**.

Yanai et al. teaches the local and remote system including a plurality of volumes of media for storing data (fig. 1, ref. num 20 and 48), wherein the local disk system is connected to a host computer **via a first communication link** (fig. 1, ref. num 18); **a second** communications link coupling the local disk system to the remote disk system, **the first and second communication links being different** (fig. 1, ref. num 40).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the local and remote system including a plurality of volumes of media for storing data, wherein the first and second communication links are different, as taught by Yanai et al., to the system of Ohran. It would have been obvious for such modifications because the plurality of volumes for storing data allow each disk system to contain a volume that is local only to their system and volumes that are accessible by the other (local/remote) system (col. 5, lines 11-34).

Claims 2-8, 18-22, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohran (USPN '307) in view of Yanai et al. (USPN '347), and further in view of Jacobson (U.S. Patent No. 5,548,649).

Regarding claims 2, 18, and 31, the combination of Ohran as modified by Yanai et al. teaches wherein the data transfer between the local disk system and the remote disk system occurring via a communication link that couples the local disk system to the remote disk system, so that the local disk system may send the data to the remote disk system without direct involvement from the host computer (see fig. 1, ref. num 16 of Ohran), wherein a first key is assigned to a first set of volumes in the local disk system, and a second key is assigned to a second set of volumes in the local disk system, each of the first and second set of volumes including one or more volumes (see col. 11, lines 53-55 of Ohran), **wherein the remote disk system is coupled to a second host computer** (see fig. 1, ref. num 52 and 54).

However, the combination of Ohran as modified by Yanai et al. does not teach further comprising a step of maintaining an encryption control table on the local disk system, the encryption control table including a list of encryption keys for selected volumes of the local and the remote disk system.

Jacobson teaches further comprising a step of maintaining an encryption control table on the local disk system (fig. 2, ref. num 232), the encryption control table including a list of encryption keys for selected volumes of the local and the remote disk system (fig. 10).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine maintaining an encryption control table on the local

disk system wherein the table includes a list of encryption keys for selected volumes of the local and remote disk system, as taught by Jacobson, to the system of Ohran as modified by Yanai et al. It would have been obvious for such modifications because the table provides a list of keys to use for encryption and decryption for the local remote system.

This new system uses a table of keys to determine how and when to encrypt and decrypt the data in the local and remote system.

Regarding claims 3 and 19, the combination of Ohran and Yanai et al. as modified by Jacobson teaches wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the local disk system (see col. 11, lines 40-43 of Ohran suggests that encryption/decryption can occur, but does not have to occur).

Regarding claims 4 and 20, the combination of Ohran and Yanai et al. as modified by Jacobson teaches wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the remote disk system (see col. 11, lines 40-43 of Ohran).

Regarding claims 5 and 21, the combination of Ohran and Yanai et al. as modified by Jacobson teaches wherein the encryption key is applicable to less than all

of the storage on the local disk system (see col. 11, lines 40-43 of Ohran shows that some, less than all, of the data is encrypted).

Regarding claims 6 and 22, the combination of Ohran and Yanai et al. as modified by Jacobson teaches wherein the encryption key is applicable to less than all of the storage on the remote disk system (see col. 11, lines 43 of Ohran shows that some, less than all, of the data is decrypted).

Regarding claim 7, the combination of Ohran and Yanai et al. as modified by Jacobson teaches wherein the encryption key is applicable to at least one disk on the local disk system (see col. 11, lines 40-43 of Ohran and fig. 1, ref. num 20 of Yanai et al. shows that the different volumes would not have to be encrypted, such as the local volume, because transmission does not occur from the local volume).

Regarding claim 8, the combination of Ohran and Yanai et al. as modified by Jacobson teaches wherein the encryption key is applicable to at least one disk on the remote disk system (see col. 11, lines 40-43 of Ohran and fig. 1, ref. num 48 of Yanai et al. shows that the different volumes would not have to be decrypted, such as the local volume, because transmission does not occur to the local volume).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH